УДК 004.4
Федоров О. – ст. гр. ІП-51м
Тернопільський національний технічний університет імені Івана Пулюя

ПРОБЛЕМИ АНАЛІЗУ ЗНІМКІВ ОПЕРАТИВНОЇ ПАМ'ЯТІ КОМП'ЮТЕРА

Науковий керівник: к.т.н., старший викладач Селін Ю.М.

Fedorov O.
Ternopil Ivan Pul'uj National Technical University

PROBLEMS OF ANALYSIS OF THE COMPUTER MEMORY DUMP

Supervisor: Selin Y.

Ключові слова: Знімки пам'яті, криміналістичний аналіз
Keywords: Memory dump, forensics

Аналіз комп'ютерної пам'яті - це аналіз знімку оперативної пам'яті комп'ютера для встановлення всіх операцій що проводились під час знімку. Він зазвичай використовується для аналізу прихованих атак на комп'ютери, коли інших артефактів не залишилося на жорсткому диску, або якщо потрібно відновити інші цінні артефакти для розслідування, такі як мережеву активність, активності всіх процесів у системі, відкриті файли, ключі шифрування (які існують тільки в енергозалежній пам'яті), і т.д.

Процес створення знімку комп'ютерної пам'яті включає в себе копіювання вмісту енергозалежної пам'яті в енергонезалежну пам'ять. Це один з найважливіших етапів в процесі криміналістичної експертизи комп'ютерної пам'яті. Якщо щось піде не так з методом збору пам'яті, знімок пам'яті може бути зіпсованим і не принести користі для аналізу. Це призведе до втрати важливих артефактів розслідування, деякі яких є незамінні (тобто які не можуть бути отримані з інших джерел), і будуть втрачені назавжди.

Знімок оперативної пам'яті комп'ютера може бути отриманий з працюючої системи з використанням різних методів, які мають власні переваги і недоліки. Деякими з них є:

- знімок з гіпервізора;
- файл сплячого режиму;
- файл аварійного знімку;
- знімок зсередини операційної системи;
- знімок спеціалізованим обладнанням.

Будь-яка активно використовувана інформація, дані, або апаратне забезпечення, буде працювати через ОЗУ під час використання системи. Це саме те, що робить аналіз оперативної пам'яті таким важливим при проведенні цифрової криміналістичної експертизи.

Артефакти оперативної пам'яті включають в себе будь-яку частину даних, які використовуються програмним забезпеченням або апаратним пристроєм. Залежно від експертизи розслідування, список можливих артефактів, отриманих з працюючого комп'ютера, може бути досить великим. Будь яке введення або виведення інформації з комп'ютерної програми буде проходити через пам'ять. Перебування інформації в оперативній пам'яті буде залежати від розміру оперативної пам'яті і необхідності

комп'ютера розміщувати нову інформацію в раніше зайнятій, але більше не використовуваній, секції оперативної пам'яті.

Сучасні операційні системи використовують такий механізм як “віртуальна пам'ять”. Він працює, надаючи кожному процесу свій власний безперервний адресний простір. Управління віртуальними адресними просторами і привласнення реальної фізичної пам'яті віртуальній пам'яті здійснюється операційною системою. З точки зору знімку комп’ютерної пам'яті це призводить до високої розрідженості сторінок пам’яті для кожного процесу.

Найбільш поширеним способом створення знімку пам’яті є використання спеціального розширення ядра, оскільки це один з найбільш часто доступних способів отримання знімків пам'яті в загальному процесі криміналістичного аналізу. Знімок пам'яті отриманий таким чином може мати внутрішні протиріччя в зв'язку з тим, що процес знімку пам'яті займає деякий час, протягом якого працююча система буде модифікувати інші частини пам'яті. Це може призвести до того, що певний об’єкт чи структура у певний час у пам’яті може бути не таким як був тоді коли на нього посилався інший об’єкт чи структура, зібраний у інший час, чи навіть зовсім не існувати. Такі невідповідності в методах збору оперативної пам'яті, заснованих на програмному забезпеченні, були описані в деяких роботах, але саме їх вплив на результати криміналістичного дослідження досі є невивченими і потребують подальшого дослідження.

УДК 004.73

Холод Д. – ст. гр. СНм-52
Тернопільський національний технічний університет імені Івана Пулюя

ВПЛИВ МОБІЛЬНОГО ЗВ’ЯЗКУ НА РОЗВИТОК ТЕХНОЛОГІЇ «РОЗУМНЕ МІСТО»

Науковий керівник: асистент Шимчук Г.В.

Holod D.
Ternopil Ivan Pul’uj National Technical University

IMPACT OF MOBILE COMMUNICATIONS ON THE TECHNOLOGY "SMART CITY"

Supervisor: assistant Shymchuk G.V.

Ключові слова: мобільний зв’язок, розумне місто, технологія
Keywords: mobile communication, smart city, technology

У найближчі десятиліття за прогнозами вчених в світі буде переважати тенденція за залучення кваліфікованих кадрів: основна конкуренція розгортається не між компаніями, а між містами. Щоб місто було конкурентним по залученню кваліфікованих фахівців, утриманню жителів і поліпшенню якості життя, системи та проекти з розвитку ”Розумного міста“ стануть критично необхідні.

Технологія «Розумного міста» є комплексом технічних рішень і процесів, які розвантажують дороги від пробок, оптимізують витрати на енергетику і роблять життя громадян значно комфортнішим. Ці рішення полягають в тому, щоб підключити